Biometric Authentication Scheme for ATM Banking System Using Energy Efficient AES Processor

Fakir Sharif Hossian*[1], Ali Nawaz [2], Khan Md. Grihan [3]

[1]Department of Electrical and Electronic Engineering, International Islamic University Chittagong, Dhaka, Bangladesh

*[1]sharifo16@yahoo.com; [2]just.piash@gmail.com; [3]grihankhan@yahoo.com

Abstract

This paper presents a highly secured ATM banking system using an optimized Advanced Encryption Standard (AES) algorithm. Two levels of security are provided in this proposed design. Firstly we consider the security level at the client side by providing biometric authentication scheme along with a password of 4-digit long. Biometric authentication is achieved by considering the fingerprint image of the client. Secondly we ensure a secured communication link between the client machine to the bank server using an optimized energy efficient AES processor. The fingerprint image is the data for encryption process and 4-digit long password is the symmetric key for the encryption process. To get a low power consuming ATM machine, an optimized AES algorithm is proposed in this paper. In this system biometric and cryptography techniques are used together for personal identity authentication to improve the security level. The design of the energy efficient AES processor is simulated in quartus-II software. Simulation results ensure its proper functionality. The realization of a demo hardware is also provided in this paper. A comparison among other research works proves its superiority.

K***eywords***

Biometric; ATM; Fingerprint; Cryptography; AES Processor; Low Power

Introduction

Nowadays security becomes a great issue in every part of life. Passing of information faces massive problems due to various types of attacks to the communication link. Many security algorithms are available to protect information from being hacked. The biometric authentication process adds a new dimension of security for any person sensitive to authentication. This paper presents a secured and an energy efficient ATM banking system that is highly secured system compared with the existing one. At present most of the ATM systems use triple data Encryption Standard (3DES). Which has some drawbacks; such as, it is vulnerable to differential attacks and also slow in performance. This paper presents security in two ways in which both the fingerprint image for the client side security and the AES algorithm for the secured communication in between. Based on these perspectives, Advanced Encryption Standard was accepted as a FIPS standard in November 2001, after which AES became the most popular encryption standard all over the world. A lot of researchers are working to improve the speed of AES as well as the other aspects like area, latency, power etc. To make the AES faster and securer, some researchers introduced hardware realizations and s-box optimizations. Today most of the researchers involving the execution of the Advanced Encryption Standard (AES) algorithm are fallen into three areas: ultra-high-speed encryption, very low power consumption, and algorithmic integrity. Many research works have been done by different hardware realizations using ASIC and FPGA technology. Some references of this paper present the energy efficient FPGA realization of the AES algorithm. This paper also focuses on biometric authentication for the client by capturing figure print image which provides another dimension of security. Fingerprint based authentication is more secure, reliable and standard than the password based authentication. Finger-scan biometric is based on the distinctive characteristics of the human fingerprint. Our existing ATM system is password based whose limitation is that its identification is inclusive to card and password, as well as the insecurity of the communication link which has access to be hacked. The proposed ATM system is able to overcome this type of limitations because proposed ATM system is fingerprint based.

Here fingerprint is used as password which is encrypted by algorithm. This encrypted process is called Cryptography, the technique, method, process and science of hiding data that plays an important role in ensuring of information security. The encrypted data is decrypted by using same algorithm and matched with the stored data. If the data matched, the access will be granted otherwise access will be denied. The simulation result is provided for the energy efficient AES processor. A comparison among other research works is also presented.

Background

ATM, the abbreviation of "Automated Teller Machine" allows the account holder to have transactions with their own accounts without the opportunity to access the entire bank's database. The idea of self-service in retail banking was developed through independent and simultaneous efforts in Japan, Sweden, the United Kingdom and the United States. In the USA, Luther George Simjian has been credited with developing and building the first cash dispenser machine. The first cash dispensing device was used in Tokyo in 1966.

FIG. 1 A CONVENTIONAL ATM SYSTEM

ATM first came into use in December 1972 in the UK. Fig. 1 shows a conventional ATM system. IBM 2984 was designed for request of Lloyds Bank. ATM is typically connected directly to their hosts or ATM Controller via either ADSL or dial-up modem over a telephone line or directly via a leased line. For transaction security, all communication traffic between ATM and transaction process is encrypted by cryptography. Nowadays most of ATM use a Microsoft OS primarily Windows XP Professional or Windows XP Embedded or Linux.

Fingerprint

Fingerprint is a characteristic unique for each person of which contains unique identifiable piece of information. The uniqueness in each fingerprint is due to the peculiar genetic code of DNA in each person. Ridges and valleys are the parts of fingerprint that provide friction for the skin. The direction and location of ridges make the identification. A fingerprint in its narrow sense is an impression left by the friction ridges of a human finger. In a wider use of the term, fingerprints are the traces of an impression from the friction ridges of any part of a human. There are three types of fingerprint patterns.

AES Algorithm

The Rijndael algorithm referred to as the AES Algorithm, is a symmetric key block cipher that can process data blocks of 128 bits, using cipher keys with lengths of 128, 192, and 256 bits. Fig. 2 shows that AES has four stages required for every round except that the last round excludes the mix column phase and the first round has only key addition. The four stages of Rijndael algorithm (AES algorithm) are:

Substitute bytes: This function uses an S-box to perform a byte-by-byte substitution of the block. For encryption and decryption, this function is indicated by SubBytes () and InvSubBytes () respectively.

Shift rows: This is a simple permutation. For encryption and decryption, this function is indicated by ShiftRows () and InvShiftRows () respectively.

Mix Columns: This is a substitution that makes use of arithmetic over GF (2^8), with the irreducible polynomial $m(x) = x^8 + x^4 + x^3 + x + 1$. For encryption and decryption, this function is indicated by MixColumns () and InvMixColumns () respectively.

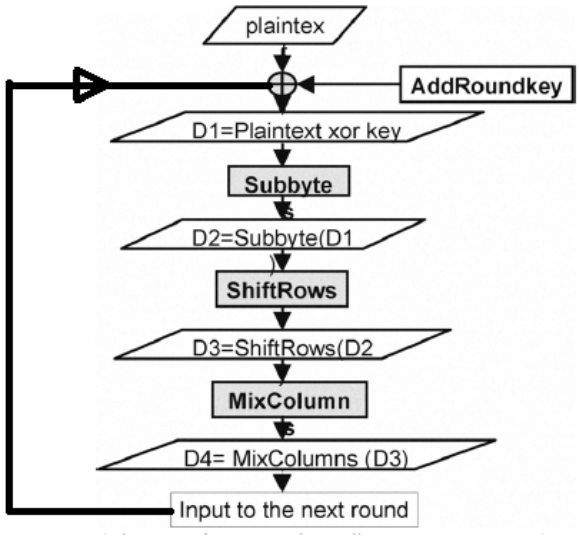


FIG. 2 AES ENCRYPTION AND DECRYPTIONS

Add round key: This function does a bitwise XOR operation of the current block with a portion of the expanded key. For both encryption and decryption this function is indicated by AddRoundKey (). For the AddRoundKey () stage, the inverse is achieved by

XORing the same round key to the block, using the result: A ⊕ A ⊕ B = B.

Design Considerations

In this section, the design consideration of proposed ATM system is presented to achieve highly secured and low power consumed ATM system. Two basic designs considered throughout this paper are biometric authentication (fingerprint) and cryptography (AES).

Fingerprint Design

The fingerprint of client taken with a image capturing device is processed over a numerous steps to get hexadecimal data. Some considerations are taken to achieve higher security for this ATM.

Original Image: The image is acquired using capturing device inside of which contains a sensor and a LED, continuously light. When an object is pressed on the image capturing portion the light intensity becomes high and the sensor senses the situation and deliveries the signal to CPU instructs the device to capture image. Fig. 3 shows the captured fingerprint images. This image is processed step by step to get a noise free actual data.

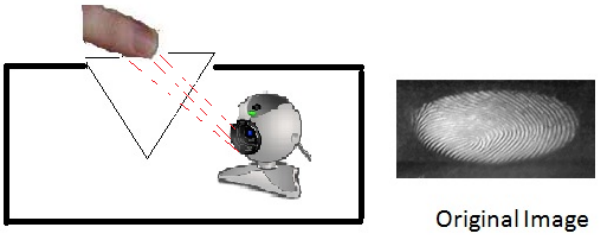


FIG. 3 IMAGE CAPTURING PROCESS & CAPTURED IMAGE

Threshold Image: Threshold condition is the simplest method of image segmentation. This process executes every pixel of the image and only counts those pixels for threshold in which pixel is more than 129. The simplest segmentation method separates out regions of an image corresponding to objects which we want to analyse. This separation is based on the variation of intensity between the object pixels and the background pixels. This threshold operation can be expressed as :(The image is an array) in Equ. 1.

$$\mathtt{dst}(x,y) = \begin{cases} \mathtt{maxVal} & \text{if } \mathtt{src}(x,y) > \mathtt{thresh} \\ 0 & \text{otherwise} \end{cases}$$

EQU. 1

Fig. 4 shows that the original image is converted to hex values by the processes. After the threshold process, the threshold image is found whose data is provided in Fig.4.

Original Image		
120	131	169
130	125	150
110	136	128
187	205	129
177	115	196

⇨

Threshold Image		
	131	169
130		150
	136	
187	205	
177		196

Threshold Image

FIG. 4 THRESHOLD PROCESS & IMAGE

Median Filter: The median filter is a nonlinear digital filtering technique, often used to remove noise with Laplacian distribution. The main idea of the median filter is to run through the signal by each entry, which is replaced with the median of neighbouring entries. After threshold there may be some noise in the image.This process executes every noise and removes all the noises from the image. The image will be smooth noise free and full qualify. Fig. 5 gives an idea about the median filtered image. The median filter is an effective method that can suppress isolated noise without blurring sharp edges. Specifically, the median filter replaces a pixel by the median of all pixels in the neighbourhood expressed by Equ. 2:

FIG. 5 MEDIAN FILTERED IMAGE

$$y[m,n] = median\{x[i,j],(i,j) \in w\}$$

EQU. 2

Where w represents a neighbourhood cantered around location (m, n) in the image.

Projected Area: After median filtering, a smooth, noise free image which is ready for process is assumed to be processed as the total area. Therefore to fix up the projected area, a boundary line is put on original image. The original image with the boundary line is the projected area. Fig. 6 shows the projected area with boundary line.

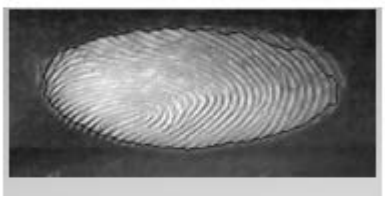


FIG. 6 PROJECTED AREA

Rotate & Cropped: Align the major axis parallel with X axis taking only the fingertip part of the image. The

image in elliptical shape, has a major and minor axis. To process the image properly, the image's major axis should be on X axis. To create the position, the major axis as X axis, at first counts the value of angle difference between the image's major axis and X axis then rotates the major axis reversed as the value of angle difference.

FIG. 7 ROTATED & CROPPED IMAGE

Fig. 7 illustrates the final image that being rotated and cropped. To extract a rectangular portion of an image, the imcrop function is utilized. Finally the image will be a specific at position and portion for use.

Edge of Ridge: This is the last step. For Canny algorithm, the object finds edges by looking for the local maxima of the gradient of the input image. The calculation derives the gradient using a Gaussian filter. Any pixel connected to a strong edge and having a magnitude greater than the low threshold corresponds to a weak edge. The Canny block computes the automatic threshold values using an approximation of the number of weak and non-edge image pixels. Fig. 8 illustrates the edge of ridge at the final stage. Using this approximation for the estimated percentage of weak edge and non-edge pixel (used to automatically calculate threshold values) parameters, this algorithm performs more robust to noise and more likely to detect true weak edges.

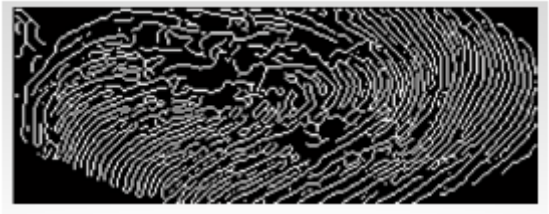


FIG. 8 EDGE of RIDGE

Low Power Design of AES Processor

To get low power AES processor, the overall power consumption of the ATM system, the S-box implementation in Galios Field $(2^4)^2$ instead of GF (2^8) has been proposed. S-box is the most costly transformation in AES, on the aspect of both time and area. Rijme suggested an alternative approach to calculate multiplicative inverses in S-Box. Since then, the relevant research has proved that the composite field $GF(2^4)^2$ based arithmetic provides the least gate count and the shortest critical path to calculate multiplicative inverse of a byte, which is the key step in S-Box. This conversion involves an isomorphic map function before and after inversion in each round. In this design it takes 128-bit key for the AES processor. Therefore it needs ten map functions for each block (128-bit) from finite field to composite field and ten inverse map functions for encryption. In addition, the key generator having S-Box includes another ten mapping and ten inverse mapping. Fig. 9 shows the mapping of $GF\ (2^4)^2$.

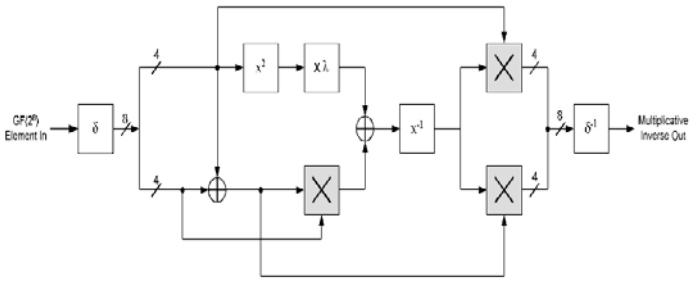


FIG.9 MULTIPLICATIVE INVERSION MAPPING IN $GF\ (2^4)^2$

To save the overhead caused by mapping, this design converts the whole AES algorithm from $GF(2^8)$ to $GF(2^4)^2$, which needs only one forward mapping before the initial round and one backward mapping after the final round. Beside this only one forward mapping is needed for the key schedule.

Proposed System and Performance

Proposed System

The proposed system consists of a fingerprint-capturing device, which captures image of the client. Taken image is fed to the image-processing device within the ATM machine. The processed image is converted to 1024 bit of binary data which is the input data of the AES processor encrypting the data with the help of 4 digit decimal key that is provided by the user as password. The data is encrypted and passed to the bank server through a communication link. At the bank side, the received cipher message is decrypted with the help of same key. The original image is reproduced at this step. Then the decrypted image of fingerprint is matched with the previously stored image of the authentic customer for the specific request of the client. If the request is valid then an acknowledgement message is sent to the ATM machine through the same communication link. If the acknowledgement is "Yes" the client can withdraw

money from the ATM machine. If acknowledgement is "No" an error message is shown on the screen of the ATM machine. In this paper we design an acknowledgement device which switches on a green light if the acknowledgement is "Yes" otherwise it turns on a red light. Fig. 10 shows the proposed ATM system.

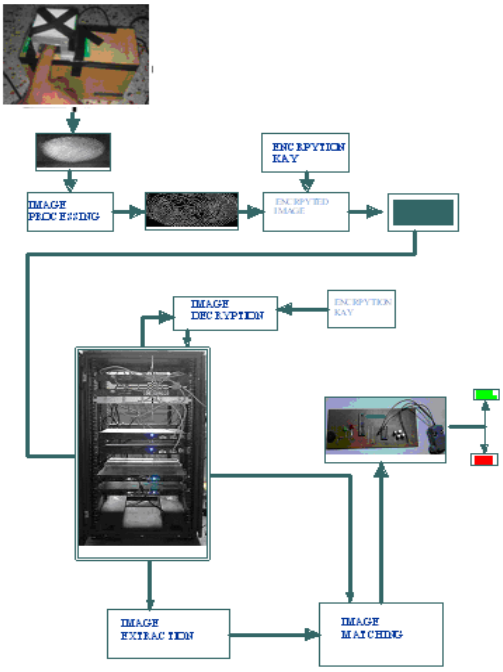


FIG. 10 PROPOSED ATM SYSTEM

Hardware Implementation

This proposed system has two hardwires; firstly an image acquisition device illustrated in Fig. 11 which consists of a prism and webcam both mounted on a wooden box. The main function of this device is to capture the fingerprint and send it to the processor for processing.

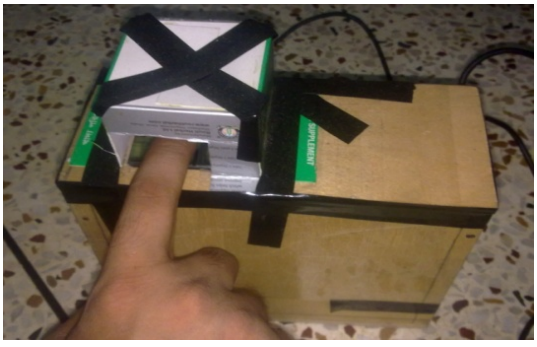


FIG. 11 IMAGE ACQUISITION DEVICE

The acknowledgement device provides the results if the matching processes are accurate. Fig. 12 shows the microcontroller based acknowledgement device which contains a red LED and a green LED. The communication link delivers the data to the main server. The processor sends the matching result serially into the microcontroller driven acknowledgment device through the serial port. If the stored image and the decrypted image match, the acknowledgment device turns on the green LED and the user can have access to his or her account. On the other hand if the acknowledgement is negative, it turns on red LED. Consequently the access will be denied.

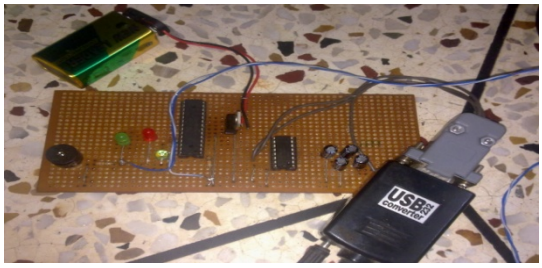


FIG. 12 ACKNOWLEDGEMENT DEVICE

Performance

The proposed system is one of the most secured and least energy consumed systems compared to the world's existing ATM systems. There are two reasons; firstly acquisition device captures image accurately. The error of the device is negligible. Secondly using AES makes the system more secured and energy efficient. The fingerprint image is processed to get the hexadecimal number values which are discussed earlier in the Section 'design consideration'. The values that come out from image processing section are the input data of the AES processor. Fig. 13 shows the simulation result for the full encryption module revealing that the cipher output comes after 9 cycles from the encryption ready flag. So the latency of this processor is 9.

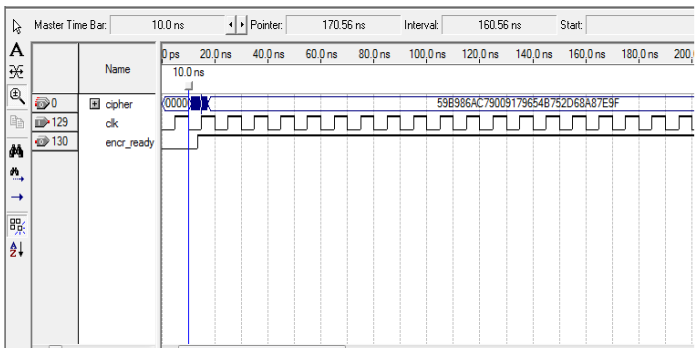
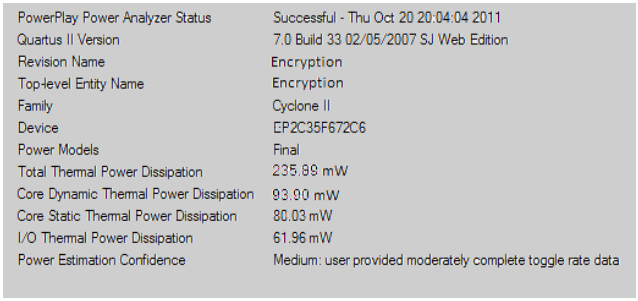


FIG. 13 SIMULATION RESULT FOR AES ENCRYPTION PROCESSES.

Fig. 14 shows the total power output of encryption processes. Here total estimated power is around 236

mW where core dynamic thermal power dissipation is approximately 94 mW.



PowerPlay Power Analyzer Status	Successful - Thu Oct 20 20:04:04 2011
Quartus II Version	7.0 Build 33 02/05/2007 SJ Web Edition
Revision Name	Encryption
Top-level Entity Name	Encryption
Family	Cyclone II
Device	EP2C35F672C6
Power Models	Final
Total Thermal Power Dissipation	235.89 mW
Core Dynamic Thermal Power Dissipation	93.90 mW
Core Static Thermal Power Dissipation	80.03 mW
I/O Thermal Power Dissipation	61.96 mW
Power Estimation Confidence	Medium: user provided moderately complete toggle rate data

FIG. 14 POWER ESTIMATION BY PPP ANALYZER

Dynamic power consumed by the encryption process is compared to the other related work in Table 1and found the superiority over other research works.

TABLE 1 COMPARISON WITH OTHER RELATED WORKS

Design	**Device**	**Static Power (mW)**	**Dynamic power (mW)**
Alam	Virtex II	80	821
Xinmiao Zhang	Virtex 4	80	125
Kenny D	Cyclone II	80.03	192.34
This work	Cyclone II	80.09	93.90

Conclusion

Biometric authentication scheme for ATM banking system using energy efficient AES processor is presented in this paper. A number of novel design considerations have been taken in designing the ATM system. It is capable safeguard against all known attacks. The whole system is simulated in quartus-II software. The simulation result shows the proper functionality of the system. The hardware implementation also carried out by implementing the LED based signaling. The encrypted message is sent to the server and compared with the stored fingerprint image. If the decrypted image and stored image is matched together, then a green LED turns on, otherwise a red LED is alight. The hardware also shows the proper functionality of the system. This design is also compared with the other research work.

REFERENCES

Alam, M., Badawy, W. and Jullien, G. "A novel pipelined threads architecture for AES encryption algorithm," Application-Specific Systems, Architectures and Processors, 2002. Proceedings. The IEEE International Conference on, pp. 296-302, 2002.

Ali, L., Roy, N. and Faisal, F. E. "Design of a High Speed and Low Latency Crypto-processor ASIC" Semiconductor Electronics, 2008. ICSE 2008.

Chandrakasan, A., Bowhill, W. "Design of High–Performance Microprocessor Circuits", (IEEE Press) 2001.

Dyken, J. V. and Delgado-Frias, J. G. "FPGA schemes for minimizing the power-throughput trade-off in executing the Advanced Encryption Standard algorithm" School of Electrical Engineering and Computer Science, Washington State University, Pullman, WA 99164-2752, USA, Available online 16 December 2009

Federal Information Processing Standards Publication (FIPS PUB) 197, National Institute of Standards and Technology (NIST). (2001, November). Advanced encryption standard (AES). Available: http://csrc.nist.gov/publication/drafts/dfips-AES.pdf.

Gaj, K. and Chodowiec, P. "Fast Implementation and Fair Comparison of the Final Candidates for Advanced Encryption Standard Using Field Programmable Gate Arrays", CT-RSA 2001, LNCS 2020, pp. 84-99, 2001.

Hodjat, A. and Verbauwhede, I. "A 21.54 Gbits/s Fully Pipelined AES Processor on FPGA", 12th IEEE Symposium on Field-Programmable Custom Computing Machines (FCCM 2004), pages 308-309, IEEE Computer Society, 2005.

IEEE Transaction on Very Large Scale Integration (VLSI) System, Vol. 12, No. 9, September 2004 957 High-Speed VLSI Architectures for the AES Algorithm Xinmiao Zhang, Student Member, IEEE, and Keshab K. Parhi, Fellow, IEEE.

Jarvinen et al, "A fully pipelined memoryless 17.8 Gbps AES-128 encryptor", International Symposium on Field Programmable Gate Arrays, pp. 207-215. 2003.

Joarvinen, K. "study on high-speed hardware implementation of cryptographic algorithm" Department of Signal processing and Acoustics, Helsinki University of technology, 10 Feb 2009.

Kenny, D., "Energy Efficiency Analysis and implementation of AES on an FPGA", Waterloo, Ontario, Canada, 2008.

Milligan, Brian (25 June 2007), "The man who invented the cash machine", BBC News, Retrieved 26 April 2010.

Morioka, S. and Satoh, A. "An Optimized S-box Circuit Architecture for Low Power AES Design", Cryptographic

Hardware and Embedded Sys. 2002, 2002, LNCS, vol. 2523, pp. 172–86.

Nachiketh, R., Potlapally, A. R." A Study of the Energy Consumption Characteristics of Cryptographic Algorithms and Security Protocols," IEEE transaction on mobile computing, vol. 5, no. 2, February 2006.

Perrig, A., Wen, V. et al, "SPINS: security protocol for sensor networks," Wireless Network", 2002, 8(5), pp. 521-534.

Saggese et al, "An FPGA-Based Performance Analysis of the Unrolling, Tiling, and Pipelining of the AES Algorithm", FPL 2003, LNCS 2778, pp. 292-302, 2003.

Satoh, A. et al, "A Compact Rijndeal HardWare Architecture with S-box Optimization" ASIACRYPT 2001, LNCS 2248, pp. 239-154, 2001.

Selvaraju, N. and Sekar, G. "A Method to Improve the Security Level of ATM Banking Systems Using AES Algorithm" International Journal of Computer Applications (0975 – 8887) Volume 3 – No.6, June 2010

Standaert et al, "Efficient Implementation of Rijndael Encryption in Reconfigurable Hardware: Improvements and Design Tradeoffs". CHES 2003, LNCS 2779, pp. 334-350, 2003.

Fakir S. Hossain was born in Dhaka, Bangladesh in 1984. He received his B. Sc. in Electrical and Electronic Engineering (EEE) from AUST in 2007. He also received his Post Graduate Diploma in Information Technology (IT) from University of Dhaka in 2009. He received his M. Sc. in Information and Communication Technology (ICT) from BUET, Bangladesh in 2012. Currently he is working as a Lecturer in the Department of Electrical and Electronic Engineering at IIUC (Dhaka Campus). His areas of interest include Cryptography, Renewable Energy, Network Security, VLSI and Embedded system design.

Ali Nawaz was born in Khulna, Bangladesh in 1990. He received his B. Sc. in Electrical and Electronic Engineering from IIUC (Dhaka Campus), Bangladesh in 2012. He also completed Cisco Certified Network Associate course in AIUB. Currently he is working as a Design & IT engineer in ElectroMech Automation & Engineering Ltd. His areas of interest include Network Security, Cryptography, Automation.

Khan Md. Grihan received his B.Sc. in Electrical and Electronic Engineering from International Islamic University Chittagong (Dhaka Campus), Bangladesh in 2011. Now he is doing his MBA in University of Dhaka, Bangladesh in 2012. Currently he is working as an Automation engineer in ElectroMech Automation & Engineering Ltd. His areas of interest include Microcontroller, Cryptography, Automation, and Renewable Energy.